protecting industrial networks

Innominate
Security Technologies

mGuard Device Manager

Release Notes
Version 1.6.2

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin
Germany
Phone: +49 30 921028 0
Fax: +49 30 921028 020
contact@innominate.com
http://www.innominate.com/

Copyright © 2006-2015 Innominate Security Technologies AG

November 2015

“Innominate” and “mGuard” are registered trademarks of Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

All information contained in this documentation is subject to change without previous notice. Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes. In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: I15028_en_00

Table of Contents

1. Introduction....3
1.1. System Requirements....3
2. Version History....3
2.1. Bug Fixes in mdm 1.6.2....3
2.2. Enhancements and Bug Fixes in Windows Installer 1.6.2.0....3
2.3. Bug Fixes in mdm 1.6.1....4
2.4. Major Enhancements since mdm 1.5.*x*....4
2.5. Security Fixes....4
3. Upgrading from mdm 1.5.*x* or Earlier 1.6.*x* Versions....4
4. Usage Hints....5
4.1. Performance of Creating Configuration History Entries....5
4.2. Caching Behavior of the mdm Server....5
4.3. Default Values....5
4.4. Device Credentials / Replacement of Devices....5
4.5. Effect of Changing Templates....6
5. Known Issues and Limitations....6
5.1. mdm Does Not Validate Variable Values as Rigidly as the mGuard....6
5.2. Support for rs2000 3G Devices....6
5.3. Concurrent Access to Templates and Pools....6
5.4. JRE Uses IPv4/IPv6 Dual Network Stack....6
5.5. JRE Prevents Usage of AES-256 Cipher by Policy....6
5.6. Change from Firmware 7.4 to 7.5....6
5.7. Exhausted Pools May Cause Unexpected Errors....7
5.8. Limitations of Referenced Table Variables....7
5.9. Changing Meshed VPN Configuration Is Slow....7
5.10. PKCS#12 Files Must Be Password Protected....7
5.11. Automatic Configuration of the VPN Peer Device....7
5.12. rs2000 Devices Cannot be Used as a VPN Peer Device....8
5.13. Server Preferences Cannot Be Removed....8
5.14. Local Time Zone....8
5.15. Microsoft Windows Installer Does Not Set Up Pull Configuration Feedback....8
5.16. Do Not Change Passwords of Windows and Database User 'postgres' (Ref. 14017)....8
5.17. Local/Remote 1:1 NAT Get Lost When Switching Device Version from 8.0 to 8.1 (Ref. 14681)....8
5.18. Diffie-Hellman Group Cannot be Configured for ISAKMP SA (Ref. 14413)....9
5.19. VPN Deactivation Timeout Applied to the Peer Device in a 1-to-N VPN Scenario (Ref. 14879)....9
5.20. 1-to-N VPN Scenario, Central VPN Gateway Becomes Unusable when the Field Devices Use Firewall Rulesets in the VPN Firewall (Ref. 14888)....9
5.21. The Value for "Accessible via" Is Not Copied to a Reconstructed Device (Ref. 15374)....9
6. Known mGuard Issues....9
6.1. mGuard Rejects Configurations For Older Firmware Versions....9
6.2. VPN Connections with Pre-Shared Secret Authentication....9
6.3. VPN Configuration Managed by Netadmin User....10
6.4. Firmware Upgrade Incorrectly Reported as Erroneous....10
6.5. mdm Cannot Read Flash ID from Guard during SSH Upload....10
6.6. Firmware Upgrade with Automatic Target Version Selection....10
6.7. SSH Upload Connection Terminated during VPN Reconfiguration....10

1. Introduction

mGuard Device Manager (mdm) 1.6.2 supports all mGuard devices running firmware versions 5.0.*x*, 5.1.*x*, 6.0.*x*, 6.1.*x*, 7.0.*x*, 7.1.*x*, 7.2.*x*, 7.3.*x*, 7.4.*x*, 7.5.*x*, 7.6.*x*, 8.0.*x*, or 8.1.*x*.

1.1. System Requirements

	mdm Client	mdm Server	mdm CA
Hardware	• A minimum of 512 MB RAM • 500 MB free hard disk space • Color monitor with at least 1280×1024 resolution	• A minimum of 4 GB RAM • 100 GB free hard disk space	• A minimum of 512 MB RAM • 5 GB free hard disk space
Software	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • Java Runtime Environment JRE SE 7	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • Java Runtime Environment JRE SE 7 • PostgreSQL Version 9.0 (or later)	• Windows 2000 SP2 / XP (or later), Windows Server 2003 (or later), or Linux • Java Runtime Environment JRE SE 7 • PostgreSQL Version 9.0 (or later)

2. Version History

2.1. Bug Fixes in mdm 1.6.2

- A bug has been fixed that caused erroneous history entries so that the server could not be started or editing a device with redundancy enabled failed.
- Several issues have been addressed that caused the unexpected locking of devices and templates if several users were working with mdm concurrently.
- A bug has been fixed that caused incorrect states for the “C” column in the mdm client for a device if an indirectly inherited template was edited.

2.2. Enhancements and Bug Fixes in Windows Installer 1.6.2.0

- The HTTPS server certificate can be replaced without re-installing the complete mdm.
- Several improvements were made regarding the handling of the values for the HTTPS and CA certificate.
- A bug has been fixed that caused the installer to fail if space characters were used in values for the HTTPS or CA certificate.
- A bug has been fixed that caused pull configuration to fail if the hostname of the mdm server was used as pull config server on mGuard devices.
- A bug has been fixed that caused the installation to fail if Windows was configured to use file names in “8.3” notation. The user is now forced to disable this notation.

- A bug has been fixed that caused the installer to exit with code 1002, even if the installation was successful.
- A bug has been fixed that caused mdm services not to be shown as running, even if they were running.
- Third party tools were upgraded to PostgreSQL 9.2.14, Apache 2.4.16, Java 7 update 80, and openssl 1.0.1p.

2.3. Bug Fixes in mdm 1.6.1

- A bug has been fixed that could cause invalid mGuard configuration files to be generated. Such configuration files were rejected by the mGuards.
- A bug has been fixed that caused changes in a template from which devices inherit indirectly (i.e. through one or more intermediate templates) not to become effective immediately.

2.4. Major Enhancements since mdm 1.5.*x*

- mdm now supports firmware versions 8.0.*x* and 8.1.*x*.
- Multiple mdm clients using an mdm server instance concurrently are now fully supported.

2.5. Security Fixes

mdm Windows Installer 1.6.0.0 and later versions include fixes for the following security vulnerabilities:

- CVE-2014-0160 (OpenSSL “Heartbleed” data leakage vulnerability)
- CVE-2014-0224 (OpenSSL SSL/TLS MITM vulnerability)
- CVE-2014-3513 (OpenSSL SRTP memory leak)
- CVE-2014-3567 (OpenSSL session ticket memory leak)
- CVE-2014-3566 (“POODLE” vulnerability)

3. Upgrading from mdm 1.5.*x* or Earlier 1.6.*x* Versions

To upgrade to mdm 1.6.2, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an earlier mdm/IDM version.

- **Preparation**
  - Stop the mdm/IDM server if it is running.
  - Dump the content of the mdm/IDM database. The command line tools `pg_dump` or `pg_dumpall` (part of the PostgreSQL distribution) or another mechanism can be used for this. See the PostgreSQL documentation for details.
  - If the mdm/IDM CA is used, dump the content of the CA database.
  - It is strongly advised to keep a copy of the database dumps as a backup.
- **Upgrade**
  - Install the mdm 1.6.2 server.

- mdm 1.6.2 requires the Java SE 7 Runtime Environment (JRE). Make sure the *java* command refers to a JRE of this version, or use an appropriate pathname to run a Java SE 7 JRE.
- Invoke the server with the following command:

  ```
  java -Xmx1024m -jar idm_server.jar update preferences.xml
  ```

  The server will connect to the PostgreSQL database, upgrade it, and terminate. After this step, the database is ready to be used by mdm 1.6.2, i.e. the mdm 1.6.2 server can now be started.

4. Usage Hints

4.1. Performance of Creating Configuration History Entries

mdm 1.6.2 creates a configuration history entry for each affected device after every modification to a device, template, or VPN group configuration. Such a modification can therefore be slow, especially if it affects a large number of devices. Further improvements to this process will be made in future mdm versions.

4.2. Caching Behavior of the mdm Server

Any RAM available to the mdm server beyond what it requires is used to cache data. It is therefore normal behavior if the memory usage increases to the configured maximum as soon as there is some activity, and subsequently remains on that level.

4.3. Default Values

If a setting is not configured in mdm, the factory default setting is assumed. It is therefore strongly recommended to configure the mGuard passwords in mdm (mGuard configuration » Authentication » Administrative Users » Passwords). Otherwise, mdm will set them to the factory default passwords.

If SSH configuration uploads from mdm are to be performed via the mGuards' external interfaces, shell access must be configured to allow connections from mdm to the mGuards (mGuard configuration » Management » System Settings » Shell access). No such access is allowed by default. Innominate recommends to configure shell access as restrictive as possible.

4.4. Device Credentials / Replacement of Devices

The “Set Current Device Credentials” dialog in the context menu of the device overview table refers to mdm's notion of the device's current passwords and should be used if the passwords have been modified by external means (e.g. through the device's web interface). To change the passwords with mdm, use the Template or Device configuration dialog (mGuard configuration » Authentication » Administrative Users » Passwords) instead.

When a device is physically replaced by a new one with factory default settings, some preparation is necessary before SSH uploads can be performed to the new device. First of all, out of security considerations mdm refuses to upload to a device if its SSH host key has changed, so the host key has to be reset. Secondly, mdm's notion of the device's passwords has to be set to the factory defaults. These steps can be performed in the “Set Current Device Credentials” dialog in the context menu of the device overview table. Check the “root”, “admin”, and “Reset SSH Host Key” boxes and type the “root” and “admin” passwords into the respective fields.

4.5. Effect of Changing Templates

Configuration values that override values in a VPN connection inherited from an ancestor template are retained as long as the ancestor template is assigned. If it is deassigned, or another parent template is assigned, overridden configuration values are lost. Likewise, pool values change when another parent template is assigned.

5. Known Issues and Limitations

5.1. mdm Does Not Validate Variable Values as Rigidly as the mGuard

Issue: mdm accepts invalid combinations of variable values that the mGuard rejects.

Solution: When an mGuard rejects a configuration, inspect the error messages generated by the mGuard and replace the invalid values with valid ones.

5.2. Support for rs2000 3G Devices

Issue: mdm does not support rs2000 3G devices as a separate hardware flavor.

Solution: Use hardware flavor “rs2000” for such devices. Set the network mode to “Router”.

5.3. Concurrent Access to Templates and Pools

Issue: If a user creates a template while another user is editing a pool, the template cannot be edited until the pool is closed. Likewise, if a user creates a pool while another user is editing a template, the pool cannot be edited until the template is closed.

Solution: Wait until the concurrently edited pool or template has been closed by the other user.

5.4. JRE Uses IPv4/IPv6 Dual Network Stack

Issue: The Java Runtime Environment uses an IPv4/IPv6 dual network stack be default. This can cause long delays (several minutes) in an IPv4-only environment. A typical phenomenon is that the mdm client appears to hang after connecting to the mdm server.

Solution: Add `-Djava.net.preferIPv4Stack=true` to the Java command line to start the mdm server, client, and CA server.

5.5. JRE Prevents Usage of AES-256 Cipher by Policy

Issue: The Java Runtime Environment has a default policy that prevents Java programs from using the AES-256 cipher. This affects encrypted configuration profiles and ECS files, which mdm encrypts with AES-128 if it is prevented from using AES-256. Note that the generated files are fully interoperable, but only have the limited crypto strength.

Solution: Download unrestricted policy files from

http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

and install them according to the instructions provided by Oracle.

5.6. Change from Firmware 7.4 to 7.5

Issue: The variable “Network Mode” with the possible values “Stealth”, “Router”, “PPPoE”, “Modem” … and the variable “Obtain external configuration via DHCP” have been replaced with

the variable “Network Mode” with the possible values “Stealth” or “Router”, and the variable “Router Mode”. Although this change has been made in mGuard firmware 7.0.0, mdm implements it for firmware 7.5 or newer.

If one of the original variables is defined in a template and the other in an inheriting template or device, the mapping may cause unexpected results, especially if one of the special “Local” or “None” values is involved.

Solution: When changing firmware version 7.4 to 7.5 in mdm, make sure the variables are both defined or both inherited, or adapt the configuration after changing the firmware version.

5.7. Exhausted Pools May Cause Unexpected Errors

Issue: If a pool is exhausted, the may cause unintelligible error messages. Affected devices may become invalid.

Solution: Extend pools before they are exhausted.

5.8. Limitations of Referenced Table Variables

Issue: If a table with content that is referenced from elsewhere (e.g. firewall rulesets) is switched from “Inherited” to “Custom”, referencing variables (e.g. targets in firewall rules) become invalid.

Solution: Set the referencing variables after switching the referenced table from “Inherited” to “Custom”.

5.9. Changing Meshed VPN Configuration Is Slow

Issue: Changing the configuration of a device that is a member of a large VPN mesh (i.e. a VPN group) can take several minutes, during which the mdm server does not respond to further requests from the client. This issue arises when the configuration change affects all devices in the mesh, so that history entries for all of them are generated.

Solution: Wait until the history entries have been written.

5.10. PKCS#12 Files Must Be Password Protected

Issue: Machine certificates in PKCS#12 format can only be imported if the PKCS#12 file is protected by a non-empty password.

Solution: If it is necessary to import a machine certificate stored in an unprotected PKCS#12 file, convert it to PEM format first (as described in the User's Manual).

5.11. Automatic Configuration of the VPN Peer Device

Issue: The automatic addition of VPN connection settings to a specifiable “peer device” only works if the peer device has the same or a newer firmware version than the originating device. Otherwise, the VPN connection is silently omitted from the peer device.

Solution: Ensure that the peer device has the same or a newer firmware version than the originating device. It is recommended not to make use of the “peer device” feature, but to use the VPN tunnel group feature.

5.12. rs2000 Devices Cannot be Used as a VPN Peer Device

Issue: The automatic addition of VPN connection settings to a specifiable “peer device” does not work if the peer device has hardware flavor rs2000.

Solution: rs2000 devices are not intended as a central gateway in a 1:N VPN topology. Use another device type as the central gateway.

5.13. Server Preferences Cannot Be Removed

Issue: It is not possible to remove server configuration settings by removing them from the server configuration file *preferences.xml*. The contents of the configuration file are copied to a system-specific location upon startup, so removing entries has no effect.

Solution: To override existing settings, specify new values in the configuration file.

5.14. Local Time Zone

Issue: The Java Runtime Environment fails to recognize the local time zone under some circumstances.

Solution: If the timestamps in the logging panel do not match your system clock, set the environment variable *TZ* to the correct time zone description (e.g. *Europe/Berlin* for Central European Time) and restart the mdm server and client.

5.15. Microsoft Windows Installer Does Not Set Up Pull Configuration Feedback

Issue: If mdm is installed with the Microsoft Windows installer, and the Windows system is also used as a pull configuration server, there is no feedback to the mdm server when mGuard devices apply configurations pulled from the server.

Solution: This functionality will be provided with a future version of the mdm installer.

5.16. Do Not Change Passwords of Windows and Database User 'postgres' (Ref. 14017)

Issue: Changing the passwords of the windows user 'postgres' or the database user 'postgres' may lead to issues that the database server can not be started anymore.

Solution: Don't change the mentioned passwords. It is strongly recommended to install the mdm server on a dedicated Windows system.

5.17. Local/Remote 1:1 NAT Get Lost When Switching Device Version from 8.0 to 8.1 (Ref. 14681)

Issue: When increasing a firmware version for a device from 8.0 to 8.1 and if this device inherits its VPN 1:1 NAT values from a template that uses firmware version < 7.4, the values for those variables get lost.

Solution: Increase the template version to => 7.4 and in the template set the values "Local NAT for IPsec tunnel connection" and "Remote NAT for IPsec tunnel connection" from ">>Inherited<< [Off]" to "1:1 NAT".

5.18. Diffie-Hellman Group Cannot be Configured for ISAKMP SA (Ref. 14413)

Issue: Starting with mGuard 8.1 the Diffie-Hellman group can be specified for the ISAKMP SA. This option can not be configured for a device in the mdm that uses mGuard firmware version 8.1.

Solution: This functionality will be provided with a future version of the mdm.

5.19. VPN Deactivation Timeout Applied to the Peer Device in a 1-to-N VPN Scenario (Ref. 14879)

Issue: A specified VPN deactivation timeout in a template for the peer devices is also applied to the VPN gateway in a 1-to-N VPN scenario but not shown in the device configuration within the mdm.

Solution: If no VPN deactivation timeout shall be used on the VPN Gateway, don't configure this option until a bug fix is provided in a future version.

5.20. 1-to-N VPN Scenario, Central VPN Gateway Becomes Unusable when the Field Devices Use Firewall Rulesets in the VPN Firewall (Ref. 14888)

Issue: In a 1-to-N VPN scenario and if in the template for the field devices are firewall rulesets used for the VPN firewall than the VPN Gateway inherits an invalid firewall configuration and therefore cannot be uploaded.

Solution: Don't configure the mentioned option until a bug fix is provided in a future version.

5.21. The Value for "Accessible via" Is Not Copied to a Reconstructed Device (Ref. 15374)

Issue: If reconstructing a device with the Configuration History feature the value for “Accessible via” is not copied to the reconstructed device.

Solution: Check the device configuration afterwards and adapt the value manually.

6. Known mGuard Issues

6.1. mGuard Rejects Configurations For Older Firmware Versions

Applicable to: Firmware versions 8.1.0 to 8.1.2.

Issue: If a device's firmware version is set to 7.0, 7.1, 7.2, 7.3, or 7.4 in mdm, a push upload to a device with an actual firmware version 8.1.0 to 8.1.2 fails.

Solution: Set the device's firmware version to 7.5 or newer in mdm.

6.2. VPN Connections with Pre-Shared Secret Authentication

Applicable to: Firmware versions 7.0.0 or later.

Issue: If pre-shared secret authentication is used in a VPN connection, the local certificate must be set to “No certificate” explicitly.

Solution: Configure the VPN connection accordingly.

6.3. VPN Configuration Managed by Netadmin User

Applicable to: Firmware versions 5.0.*x* and 5.1.*x*.

Issue: If configuration variables within the “Tunnel and Transport Settings” of a VPN connection are managed by the Netadmin user on the device (i.e. set to “Local” in mdm), the values set by the Netadmin user are reset to the default values on every configuration upload or pull.

Solution: Upgrade to firmware 6.0.0 or later.

6.4. Firmware Upgrade Incorrectly Reported as Erroneous

Applicable to: Firmware versions 5.0.*x* and 5.1.*x*.

Issue: If a firmware upgrade to version 6.0.*x* is triggered by a configuration pull, the device incorrectly reports a firmware upgrade failure to mdm even if the upgrade succeeded. mdm will indicate an upgrade failure in the device overview table.

Solution: Wait until mdm receives the next configuration pull feedback from the device. This feedback contains the correct status and therefore causes mdm to no longer indicate an upgrade failure.

6.5. mdm Cannot Read Flash ID from Guard during SSH Upload

Applicable to: Firmware version 5.0.0.

Issue: If an SSH configuration upload is performed to a device with firmware version 5.0.0, mdm cannot read back the Flash ID. This prevents licenses from being associated with the device.

Solution: Enter the Flash ID manually in the device configuration dialog, or upgrade to firmware 5.0.1 or later.

6.6. Firmware Upgrade with Automatic Target Version Selection

Applicable to: Firmware versions 5.0.*x,* and 5.1.*x*.

Issue: Firmware upgrades from version 5.1.*x* or earlier with automatic selection of the target version (i.e. upgrades to latest patches, latest minor release, or next major version) are only triggered by a configuration pull if mdm knows the firmware version on the device when exporting the configuration profile. If mdm lacks this information, any scheduled firmware upgrade request remains so until the version on the device is known. Upgrades triggered by an SSH configuration upload are not affected.

Soultion: Enter the firmware version on the device manually in the device configuration dialog.

6.7. SSH Upload Connection Terminated during VPN Reconfiguration

Applicable to: Firmware versions 5.0.*x,* and 5.1.*x*.

Issue: If an SSH configuration upload changes the settings of a large number of VPN connections, mdm declares the SSH connection dead before the upload is complete.

Solution: Increase the SSH timeout values in the server configuration file `preferences.xml` when working with a lot of VPN connections.